Montana Law Review

Volume 63
Issue 2 *Summer 2002*

Article 4

7-2002

The Issues of E-Mail Privacy and Cyberspace Personal Jurisdiction: What Clients Need To Know about Two Practical Constitutional Questions Regarding the Internet

Mark S. Kende
Professor of Law, University of Montana School of Law

ARTICLE

THE ISSUES OF E-MAIL PRIVACY AND CYBERSPACE PERSONAL JURISDICTION: WHAT CLIENTS NEED TO KNOW ABOUT TWO PRACTICAL CONSTITUTIONAL QUESTIONS REGARDING THE INTERNET

Mark S. Kende*

INTRODUCTION

Cyberspace seems to reach everywhere. On a macro-level, a Canadian company could risk being subject to Montana court jurisdiction based on the company's Web site being accessible to Montanans.[1] On a micro-level, an employee's privacy is vulnerable when her company knows the contents of e-mails sent from and received at her work computer.

Many law review articles have been written on these topics.[2]

---

* Associate Professor of Law, University of Montana School of Law. B.A. Yale University. J.D. University of Chicago Law School. Special thanks to Diana Copeland and Chase Rosario for their assistance with the research, and to Mike Begley for his diligent editing.

1.*See* Bedrejo v. Triple E Canada, Ltd., 1999 MT 200, 295 Mont. 430, 984 P.2d 739 (court examines whether the Canadian manufacturer of an allegedly defective motor home can be subject to jurisdiction in Montana based in part on the company's Web site).

2.For a list of cyberspace personal jurisdiction articles, see Joseph S. Burns & Richard A. Bales, *Personal Jurisdiction and the Web*, 53 ME. L. REV. 29, 31 n.3 (2001). A list of cyberspace personal jurisdiction cases can be found in Richard E. Kaye, Annotation,

Few combine a theoretical analysis with practical recommendations regarding what attorneys should advise clients to avoid liability. Moreover, there's been little written for the Montana practitioner.[3] This article's purpose is to fill the scholarly gaps regarding these two distinct cyberspace law topics.

Part I analyzes the constitutionality of employer e-mail monitoring. This section recommends Montana employers take specific precautions before monitoring because the Montana Constitution's right to privacy, and to dignity, make such activity suspect.[4] This section also briefly examines monitoring under the U.S. Constitution's Fourth Amendment and federal privacy statutes.

Part II examines personal jurisdiction in cyberspace, focusing on decisions from the U.S. Court of Appeals for the Ninth Circuit and the Montana Supreme Court. This section assesses the popular "sliding scale" approach, which holds that non-resident Web site owners should only be subject to jurisdiction if their site is sufficiently interactive with the forum state.[5] This section also examines the "effects test," which centers on the impact of a defendant's actions.[6] The section concludes by providing specific recommendations on how clients can reduce the liability risks of having a Web site.

Internet Web Site Activities of Nonresident Person or Corporation as Conferring Personal Jurisdiction Under Long-Arm Statutes and Due Process Clause, 81 A.L.R 5th 41 (2000). One of the earliest articles on e-mail monitoring is by Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345 (1995).

3. One of the few sources is *Privacy in Cyberspace: Transcripts from the 1999 Judge James R. Browning Symposium*, 61 MONT. L. REV. 43 (2000).

4. The privacy provision is in Article II, Section 10, of the Montana Constitution and the dignity clause is in Article II, Section 4.

5. The source of the sliding scale approach is *Zippo Mfg. Co. v. Zippo Dot Com*, 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (holding Pennsylvania has jurisdiction over California Internet news provider because of defendant's contracts with 7 Pennsylvania Internet service providers and with 3000 Pennsylvania residents). *Zippo* is one of the most frequently cited cyberspace cases. *See, e.g.*, Roy N. Dreben & Johanna Werbach, *Top 10 Things to Consider in Developing an Electronic Commerce Web Site*, COMPUTER LAW., May 1999 at 19 (stating that Internet jurisdiction law is supposedly "coalescing" around the "seminal" *Zippo* case).

6. The "effects test" was born in *Calder v. Jones*, 465 U.S. 783 (1984), where the Supreme Court ruled a defendant who committed an intentional tort (defamation), whose primary damaging effect would be felt by the plaintiff in a particular state, would presumably be subject to personal jurisdiction there.

I. CONSTITUTIONAL ISSUES REGARDING E-MAIL MONITORING

In May 2001, Judge Alex Kozinski and other Ninth Circuit judges became upset when they discovered the Administrative Office of the U.S. Courts (AO) in Washington D.C. could monitor computer usage, including electronic mail, in their judicial chambers.[7] The judges, feeling their privacy rights were being violated, instructed Ninth Circuit computer staff to disconnect the AO's monitoring capacity.[8] AO officials claimed this instruction made the Ninth Circuit computers vulnerable to hackers. AO Director Leonidas Ralph Mecham even contended Judge Kozinski was "advocating his passionate views that judges are free, undetected, to download pornography and Napster music on government computers in federal court buildings on government time even though some of the downloading may constitute felonies."[9] Since then, the AO's monitoring capacity has apparently been reinstalled but with some limitations.[10]

The existence of a right to privacy under the U.S. Constitution was advocated in a famous Harvard Law Review article by Louis Brandeis and Samuel Warren at the end of the 19th Century.[11] They defined it as the "right to be left alone."[12] Even then, the authors expressed concern about new technologies such as "instantaneous photographs" and "numerous mechanical devices."[13] Today's sophisticated technologies make "spying" kid's play, particularly in an area such as workplace e-mail. The New York Times in July 2001 reported:

> a study released in the spring by the American Management Association, a New York-based management development and training non-profit, [which] concluded that more than three-quarters of major U.S. firms now spot-check their employees' phone calls, e-mails, Internet activities and computer files. The

---

7. Neil A. Lewis, *Plan for Web Monitoring in Courts Dropped*, N.Y. TIMES, Sept. 9, 2001, Late-Edition, § 1, at 34.

8. Neil A. Lewis, *Rebels in Black Robes Recoil at Surveillance of Computers*, N.Y. TIMES, August 8, 2001, at A1.

9. Lewis, *supra* note 7 (quoting Mecham, internal quotation marks omitted).

10. Tony Mauro, *Judicial Conference Approves Monitoring of Judges' Internet Use*, AMERICAN LAWYER MEDIA, Sept. 20, 2001, *available at* http://www.law.com.

11. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

12. *Id.* at 195 (citing COOLEY ON TORTS (2d. ed.) at 29).

13. *Id.* at 195.

figure has doubled since 1997, driven principally by employer concerns about liability for workplace harassment . . . .[14]

This section of the article addresses whether employers are limited by constitutional or other restraints in monitoring employee e-mail. The first part discusses U.S. Supreme Court cases. The second part surveys case law and scholarship outside of Montana. Finally, I'll describe what Montana's constitution and case law say in relation to monitoring employee e-mail. My conclusion is, although most jurisdictions have upheld employer monitoring rights, such monitoring is suspect in Montana given the State Constitution's strong privacy and dignity provisions.

A. U.S. Supreme Court Decisions

The U.S. Supreme Court's only cyberspace foray occurred in a free speech case, *Reno v. ACLU*.[15] The Court has yet to hear a cyberspace privacy case. The Court, however, has recently dealt with privacy issues involving new technologies, which provides some initial guidance.

Last term, in *Kyllo v. U.S.*,[16] the Court ruled police use of thermal imaging technology from outside a home constituted a Fourth Amendment search, meaning probable cause and warrant requirements had to be satisfied. Justice Scalia wrote, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology . . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[17] Two factors weighing heavily in Scalia's decision were the technology's unavailability to the public, and the sanctity of the home.[18]

Also last term, in *Bartnicki v. Vopper*,[19] the Court ruled the First Amendment precludes a newspaper from prosecution under the Federal Wiretap Act for publishing cellular phone

14. Carl S. Kaplan, *Reconsidering the Privacy of Office Computers*, CYBER LAW JOURNAL, July 27, 2001 *at* http://www.nytimes.com/2001/07/27/technology/27CYBERLAW. html.

15. 521 U.S. 844 (1997).

16. 533 U.S. 27 (2001).

17. *Kyllo.* at 33-34.

18. This pro-defendant ruling from a generally conservative U.S. Supreme Court surprised many experts and amounted to an implicit vindication of the Montana Supreme Court's ruling several years earlier in *State v. Siegal*, 281 Mont. 250, 934 P.2d 176 (1997).

19. 532 U.S. 514 (2001).

conversation transcripts on matters of public importance if obtained illegally by a third party. In dissent, Chief Justice Rehnquist wrote:

> Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations: (sic). . . . But the Court's decision diminishes, rather than enhances, the purposes of the First Amendment: chilling the speech of the millions of Americans who rely upon electronic technology to communicate each day.[20]

Another case relevant to the e-mail issue is *O'Connor v. Ortega,*[21] where the Court held workers have a reasonable expectation of privacy in their offices, desks, and file cabinets but the expectation may be reduced by the "operational realities of the workplace."[22]

The above U.S. Supreme Court cases involved alleged governmental intrusions on privacy. Constitutional protections, however, generally don't apply to private actors. Thus, one of the many questions to be discussed here is what privacy rights or additional constitutional guarantees do private employees retain in their work e-mail. Except perhaps in Montana, most private employees have little legal recourse.

B. Results Outside of Montana

Most courts have ruled employers can monitor worker e-mail and computers. This section initially examines relevant federal law and then looks at decisions from courts in other states. These authorities need to be discussed first to provide perspective on the later Montana analysis.

1. Federal Law

a. The Federal Constitution

The U.S. Constitution so far has not generally prevented government e-mail monitoring. For example, in *United States v.*

20. *Id.* at 541-42 (Rehnquist, C.J., dissenting).
21. 480 U.S. 709 (1987).
22. *O'Connor,* 480 U.S. at 717.

Simons,[23] the U.S. Court of Appeals for the Fourth Circuit ruled the CIA's remote warrantless search of an employee's office computer hard drive did not violate the Fourth Amendment.[24] The Court reasoned the employee knew monitoring was permitted.[25] Moreover, the CIA possessed substantial evidence indicating the employee used his office Internet connection to traffic in child pornography.[26]

b. Federal Statutes

The Federal Wiretap Act,[27] as amended by the Electronic Communications Privacy Act (ECPA), prohibits the unauthorized "interception" of "electronic communications."[28] Most courts say interception requires a party to obtain a record of the communication while it's being transmitted.[29] Similarly, the Act has historically authorized contemporaneous interception of phone conversations. Thus, under this traditional interpretation, in most jurisdictions it is legal for an employer to search an employee's hard drive for saved e-mail messages because no transmission is occurring.[30]

In *Konop v. Hawaiian Airlines,*[31] the U.S. Court of Appeals for the Ninth Circuit rejected this narrow approach. Though the Ninth Circuit ultimately withdrew the *Konop* opinion, it's worth looking at because it shows that even a liberal interpretation of ECPA's provisions provides only limited privacy protection to employees. In *Konop*, an airline pilot had a secure Web site that criticized his employer.[32] Airline company officials surreptitiously accessed the site by persuading other pilots to give them their passwords.[33] The Ninth Circuit stated the Web site owner could pursue a Wiretap Act claim based on the company's unauthorized downloading of information, even

23. 206 F.3d 392 (4th Cir. 2000). *See also* United States v. Slanina, 283 F.3d 670 (5th Cir. 2002).

24. *Simons*, 206 F.3d at 398.

25. *Id.*

26. *Id.* at 401.

27. 18 U.S.C. §§ 2510-2520 (2001).

28. *Id.* at § 2511.

29. *See, e.g.,* United States v. Turk, 526 F.2d 654 (5th Cir. 1976).

30. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994).

31. 236 F.3d 1035 (9th Cir. 2001), *opinion withdrawn*, 262 F.3d 972 (9th Cir. 2001) (the court indicates that "A subsequent opinion will be filed at a later date.") *Id.*

32. 236 F.3d at 1041. (The site attacked the labor policies of the airline).

33. *Id.*

though the downloading was not contemporaneous with any transmission.[34] The court explained:

> It would be equally senseless to hold that Konop's messages to his fellow pilots would have been protected from interception had he recorded them and delivered them through a secure voice bulletin board accessible by telephone, but not when he set them down in electronic text and delivered them through a secure web server accessible by a personal computer. We hold that the Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit.[35]

It seems, however, that *Konop*'s reasoning doesn't preclude employer e-mail monitoring because *Konop* involved illegal intrusions into the employee's secure personal Web site whereas employers generally own and control the computers and e-mail systems their employees use at work. Indeed, the 1986 ECPA provides an exception for employers.[36] The Stored Communication Act also doesn't protect most employees from monitoring because it prohibits unauthorized "access" to "a facility through which an electronic communication service is provided."[37] This is geared towards hacking, not monitoring.

In *Bohach v. City of Reno*,[38] a federal district court rejected police officer claims the department violated their privacy rights under the ECPA by accessing messages on their electronic pagers. The Court found the officers knew pager messages were placed on a department network open to those with access.[39] The Court also ruled the department qualified as a "service provider" under the ECPA and thus could access the stored messages.[40]

In 1994, Congressman Pat Williams of Montana introduced legislation in the U.S. House of Representatives designed to

---

34. *Id.* at 1044. At least one commentator has advocated such an approach. Tatsuya Akamine, *Proposal for a Fair Statutory Interpretation: Email Stored in a Service Provider Computer is Subject to an Interception Under the Wiretap Act*, 7 J.L. & POL'Y 519, 527-28 (1999).

35. *Konop,* at 1046.

36. ELLEN ALDERMEN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 315 (1995). *See also* Erik J. Belanoff et. al., *E-Mail: Property Rights v. Privacy Rights in the Workplace*, 45 PRAC. LAW., Dec. 1999, at 33. ("Accessing someone else's mailbox and reading their stored e-mail messages does not constitute an interception for purposes of a criminal violation of section 2511.").

37. 18 U.S.C. § 2701(a)(1) (2002).

38. 932 F. Supp. 1232 (D. Nev. 1996).

39. *Bohach*, 932 F. Supp. at 1233.

40. 18 U.S.C. § 2701(c)(1) (2002). This statute also has an exception which makes it legal to inspect e-mails if the "conduct [is] authorized by a user of that service with respect to a communication of or intended for that user. . . ." *See* 18 U.S.C. § 2701(c)(2).

protect worker privacy. However, the legislation never passed.[41] Since existing federal statutes don't protect employees from e-mail monitoring, it's necessary to see what the case law says regarding privacy issues in cyberspace.

2. Case Law Outside Montana

In *Smyth v. Pillsbury Company,*[42] a federal district court ruled Pillsbury did not wrongfully discharge Smyth when it fired him because of his unprofessional e-mail statements.[43] Smyth alleged a tortious invasion of privacy.[44] Indeed, Pillsbury had promised employees that all e-mail communications were confidential and unmonitored, and that no employee could be terminated based on e-mail comments.[45]

Nonetheless, in ruling for Pillsbury, the Court noted:

> Unlike urinalysis and personal property searches, we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management.
>
> Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. . .[Moreover] we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy.[46]

Smyth's reasoning has several weaknesses. One author argues the decision confused Smyth's legitimate expectation of e-mail privacy, fostered by his supervisor's statements, with the fact he admittedly did not work or communicate in solitude.[47] The author also suggests the decision conflicts with the U.S. Supreme Court's *Ortega* case, which recognized employees have

41. *See* H.R. 1900, 103d Cong., TO PREVENT ABUSES OF ELECTRONIC MONITORING IN THE WORKPLACE (1993).

42. 914 F. Supp. 97 (E.D. Pa. 1996).

43. *Smyth*, 914 F. Supp. at 99. Smyth apparently said in frustration that he'd like to kill some members of the sales force, and that a company party would be like a Jim Jones Koolaid event. *See* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 74 (2000).

44. *Id.*

45. *Id.*

46. *Smyth*, 914 F. Supp. at 101.

47. Rod Dixon, *Windows Nine-To-Five: Smyth v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communications*, 2 VA. J. L. & TECH. 4, 22 (1997).

reasonable privacy expectations in the workplace.[48] The author further explains, "Paradoxically, the privacy protection afforded postal mail and voice-mail far outstrips that currently afforded e-mail. Moreover, unlike postal mail, e-mail reaches its intended recipient almost instantaneously and may be more secure than postal mail by adopting encryption technology."[49] In addition, Professor Jeffrey Rosen argues the Court was wrong in assuming the privacy intrusion was not substantial or highly offensive, particularly given how easily outsiders can misinterpret the meaning of private e-mails.[50]

Nonetheless, *Smyth* has been followed. In *McLaren v. Microsoft Corp.*,[51] a Texas court of appeals rejected Bill McLaren's claim that Microsoft's examination of e-mail stored on his office computer's "personal folders" invaded his privacy. The court rejected McLaren's argument that his computer is similar to an employee work locker.[52] The Court reasoned the work locker is entitled to more privacy because it's intended for personal belongings, whereas the computer is for work.[53] Further, the locker is more private because "any e-mail messages stored in McLaren's personal folders were first transmitted over the network and were at some point accessible by a third party."[54] McLaren's use of a private password did not change the court's view.[55] Finally, Microsoft was inspecting the computer because of serious sexual harassment accusations against McLaren, which could expose the company to liability.[56] Thus, the company's interest in preventing illegal activity outweighed McLaren's privacy interest.[57]

An unreported California decision, *Shoars v. Epson America,* likewise rejected a privacy violation claim by an employee whose e-mail was examined. The trial court declared the e-mail messages to be mainly business related and "with few exceptions," California's state constitutional right to privacy covered only "personal information . . . no sufficient legal or

48. *Id.* at 25.
49. *Id.* at 31.
50. ROSEN, *supra* note 43, at 75.
51. No. 97-00095-F, 1999 WL 339015 (Tex. App. May 28, 1999).
52. *McLaren*, 1999 WL 339015, at *4.
53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.* at *5.
57. *McLaren*, 1999 WL 339015, at *5.

factual basis [existed] for extending the right to privacy to cover business-oriented communications."[58] Numerous other courts have discussed the limited privacy rights of employees.[59]

In contrast, the Superior Court of Massachusetts has questioned employer e-mail monitoring. In *Restuccia v. Burk Technology*,[60] a supervisor learned two of his employees had been wasting time on their computers at work.[61] These same employees also authored e-mails critical of their supervisor.[62] The supervisor discharged the employees.[63] In a rather conclusory decision, the Court decided the plaintiffs' tort claims for invasion of privacy should survive summary judgment because there were genuine issues of material fact as to "whether plaintiffs had a reasonable expectation of privacy in their E-Mail messages and whether Burk's reading of the E-Mail messages constituted an unreasonable, substantial, or serious interference with plaintiffs' privacy."[64]

Perhaps the most noteworthy defense of an employee's right to privacy in the e-mail context comes from a short law journal article published by U.S. District Judge James Rosenbaum, of Minneapolis.[65] Judge Rosenbaum acknowledges the common assumption employees lack such a right because the computer is the employer's property. However, Judge Rosenbaum then describes this country's long tradition of honoring privacy rights, going back to the founding fathers, and says:

> An employee unquestionably owes a duty to perform services on the employer's behalf during the work day.... But do the employee's idle acts permit the employer to more, beyond proof of the employee's breach of duty? After establishing its right to

58. ELLEN ALDERMAN & CAROLINE KENNEDY, IN OUR DEFENSE: THE BILL OF RIGHTS IN ACTION 315 (1998).

59. Medical Lab. Mgmt. Consultants v. ABC, Inc., 30 F. Supp. 2d 1182, 1208-09 (D. Ariz. 1998); Ali v. Douglas Cable Communications, 929 F. Supp. 1362, 1378-80 (D. Kan. 1996); People for the Ethical Treatment of Animals v. Bobby Berosini, Ltd., 895 P.2d 1269, 1281 (Nev. 1995); Cox v. Hatch, 761 P.2d 556, 563 (Utah 1988).

60. 1996 WL 1329386 (Mass. Supp. 1996).

61. *Id.* at *1.

62. *Id.*

63. *Id.*

64. *Restuccia,* 1996 WL 1329386 at *3. Two other cases asserting employees have limited privacy rights in their workplace e-mail, until it's received by someone else, are *United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) and *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996). One of the few cases to take a pro-employee perspective in the workplace privacy debate, but not involving e-mail monitoring, is *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983).

65. The piece's significance was shown by an article about it in the *New York Times*. *Kaplan*, *supra* note 14.

> reimbursement, recompense, or even termination, the employer's right to wander through the employee's personal material does not seem self-evident.[66]

He proposes that employers who wish to search an employee's computer or e-mail provide advance notice and other procedural protections to the employee.[67] Thus, even Judge Rosenbaum concedes the employer's authority to monitor, albeit with some limitations.

C. The Montana Constitution

This section looks at how the Montana Supreme Court might treat the e-mail monitoring issue under the Montana Constitution. Additionally, this section discusses how employers can prevent liability. To date, no Montana case has specifically addressed the e-mail question.

The Montana Constitution's privacy provision[68] and dignity provision[69] would likely make the analysis of e-mail monitoring different here than nationally. I will deal with each separately as well as with the scrutiny analysis that might result.

1. Privacy

Montana's privacy provision states, "The right of individual privacy is essential to the well being of a free society and shall not be infringed without the showing of a compelling state interest."[70] This privacy right has been interpreted more broadly in Montana than at the federal level. This makes sense as there is no explicit right to privacy in the U.S. Constitution. The U.S. Supreme Court had to find an implied right to privacy

66. James M. Rosenbaum, *In Defense of the Hard Drive*, 4 GREEN BAG 2d 169, 170 (2001). *See also* James M. Rosenbaum, *In Defense of the DELETE Key*, 3 GREEN BAG 2d 393 (2000).

67. Other articles raising concerns about employer e-mail monitoring include: Amanda Richman, Note, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 IOWA L. REV. 1337 (2001); Carey C. Hooper, Comment, *You've Got Mail: Privacy Rights in the Workplace*, 25 S. ILL. U. L.J. 609 (2001); Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379 (2000); Dan McIntosh, *e-Monitoring @ workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace*, 23 HAMLINE L. REV. 539 (2000); Larry O. Gantt, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345 (1995); *Dixon*, *supra* note 47.

68. MONT. CONST. art. II, § 10.

69. MONT. CONST. art. II, § 4.

70. MONT. CONST. art. II, § 10.

in decisions like *Griswold v. Connecticut*[71] and *Roe v. Wade*.[72] Moreover, unlike the U.S. Supreme Court, Montana's Supreme Court has ruled in favor of the privacy rights of homosexuals.[73] Additionally, Montana's Supreme Court supports abortion rights more strongly than the U.S. Supreme Court's most recent pronouncement in the area.[74]

It is also worth noting that Montana's privacy provision appears to cover non-governmental conduct, unlike most federal constitutional rights. However, there has not been much case law articulating how vigorously the Montana courts will apply the constitutional protections to private entities.[75]

The seminal case for the e-mail issue is *State v. Siegal*.[76] In *Siegal*, the Montana Supreme Court held police use of thermal imaging technology was a search, in large part because such technology infringed the right to privacy of those in the home.[77] The Court said the average Montanan would find it shocking to learn the government could secretly monitor homes for heat signatures without consent or a warrant.[78]

The Court explained further that the 1972 Montana Constitutional Convention adopted the privacy provision out of grave concerns about how "computerized data banks" and other modern technologies (such as wiretaps) could collect information about people without their knowledge.[79] The Court noted the problem was not only government, but also private actors with such capacities.[80] The Court therefore concluded the framers

71. 381 U.S. 479 (1965).

72. 410 U.S. 113 (1973).

73. Gryczan v. State, 283 Mont. 433, 942 P.2d 112 (1997).

74. *Compare* Armstrong v. State, 1999 MT 261, 296 Mont. 361, 989 P.2d 364 (1999), *with* Planned Parenthood v. Casey, 505 U.S. 833 (1992).

75. Alaska has a constitutional provision which expressly seems to guarantee privacy even from private party intrusions, yet the Alaska courts have limited the provision to governmental actions. Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123 (Alaska 1989). Montana, however, has already made clear in court decisions that its constitutional provisions outlaw private violations in many contexts, such as regarding environmental degradations. See Cape-France Enters. v. Estate of Peed, 2001 MT 139, 305 Mont. 513, 29 P.3d 1011; Montana Envtl. Info. Ctr. v. Department of Envtl. Quality, 1999 MT 248, 296 Mont. 207, 988 P.2d 1236. An excellent argument for finding that privacy rights should apply to private employees can be found in McIntosh, *supra* note 67, at 572.

76. 281 Mont. 250, 275, 934 P.2d 176, 190 (1997).

77. 281 Mont. at 262-63, 934 P.2d at 183.

78. *Siegal*, 281 Mont. at 274, 934 P.2d at 190.

79. *Id.* at 274, 934 P.2d at 191.

80. *Siegal*, at 278, 934 P.2d at 191-192. This history shows the argument for applying the Montana privacy provision to non-governmental actors is therefore even

would have found thermal imaging technology to be a privacy violation.[81]

The argument that unannounced e-mail monitoring violates privacy seems even stronger than for thermal imaging. Montana's framer's were expressly concerned with computerized data base intrusion back in 1972 and that's what's involved when an employer sneaks into their employee's e-mail records.

This argument finds support in a speech given at the Montana Law Review's 1999 Judge James R. Browning Cyberspace Symposium by Nancy Sinclair, a Montana attorney who represents employers on Internet and e-mail issues. As part of a panel on "Privacy in Cyberspace," Ms. Sinclair stated:

> Many companies [and] firms. . .[now] have access. . .to e-mail from outside sources. A frequently asked question is, can I read an employee's e-mail? Nationally, there is a trend towards saying, in the private sector, there is no expectation of privacy in e-mail received on an employer's computer. . .The thing about Montana is, as Professor Elison discussed, we have a heightened constitutional privacy provision. I believe that the Montana Supreme Court could easily find that employees do have an expectation of privacy in their e-mail, especially in light of the fact that many companies don't have any policies even addressing this issue.[82]

Moreover, a *Practical Lawyer* article on worker privacy specifically references Montana as a state "where an employee's right to privacy is heightened" given the specific protections found in the Montana Constitution.[83]

In response, employers can point to the Montana statute stating any property the employee acquires by virtue of his employment (except salary or other compensation) remains the employer's belonging, and presumably this would include a computer that the employee is using for personal e-mail

---

stronger than for applying some other Montana constitutional provisions. It is worthwhile to recall that in 1972, there was substantial evidence indicating the FBI and other government agents had engaged in illegal wiretapping, eavesdropping, and other activities targeted at certain political groups, such as those actively opposing the Vietnam War or supporting the civil rights movement. And as the Watergate scandal showed, even the Republican Party, technically a private entity, used such illicit tactics. This was the historical backdrop when the Montana delegates met and it explains their concerns with such technologies and privacy issues.

81. *Id.* at 278, 934 P.2d at 192.

82. *Privacy in Cyberspace: Transcripts from the 1999 Judge James R. Browning Symposium*, 61 MONT. L. REV. 43, 64 (2000).

83. Erik J. Belanoff, Evan J. Spelfogel & Maureen K. Bogue, *E-Mail: Property Rights vs. Privacy Rights in the Workplace*, PRACTICAL LAWYER, Dec., 1999, at 29, 38.

messages.[84] However, if the U.S. Supreme Court in *Ortega* found employees have privacy rights in their desk drawer contents, it seems the Montana Supreme Court would find even greater privacy rights in the e-mail situation, especially where employees have individual unpublicized passwords.

Montana has two other relevant electronic statutes, yet neither seem to undermine this constitutional analysis. One provision protects the privacy of electronic communications, though its major focus appears to be the purposeful unauthorized *interception* of data in the process of being transmitted.[85] In addition, Montana has an anti-hacking statute forbidding the unlawful use of a computer.[86]

A broader counter-argument is all employees should know e-mail is not guaranteed to remain confidential. The Monica Lewinsky scandal made this obvious.[87] Thus, employees can have no subjective expectation of privacy, nor any objectively reasonable expectation of privacy.[88] Even the e-mail's recipient could forward the e-mail on to others.[89] But this was essentially the argument made in *Smyth,* which was effectively dismantled by the critics who showed that it confused an expectation of privacy with a lack of solitude; that it paradoxically gave phone conversations more protection than e-mail; and that it ignored the true degradation involved when an employee has been monitored without knowledge. These criticisms are particularly persuasive in a jurisdiction like Montana with such strong

84. MONT. CODE ANN. § 39-2-102 (2001).

85. MONT. CODE ANN. § 45-8-213 (2001).

86. MONT. CODE ANN. § 45-6-311 (2001).

87. *See* ROSEN, *supra* note 43, at 54 (Professor Jeffrey Rosen discusses this at length). Another critique of the position that Montana employees have special e-mail privacy rights is that the federal ECPA preempts state constitutional provisions and occupies the field. There are several problems with this argument. First, a decision from a Ninth Circuit court has already rejected this kind of preemption argument. In *Roberts v. Americable Intern. Inc.*, the Court stated, "Of course, federal law will not control in state court in the face of a state statute governing the tape recording of private conversations when that state law is stricter than the federal law." *Id.*, 883 F. Supp. 499, 503 n.6 (E.D. Cal. 1995). Second, it does not appear ECPA was intended to occupy the field and eliminate state created privacy rights.

88. *Katz v. United States,* 389 U.S. 347 (1967). The *Katz* approach is particularly tempting to use here as the case involved the modern technology question of whether the government engaged in a search by wiretapping a public telephone. The *Siegal* case relied in part on this *Katz* analysis too.

89. Professor Rosen's book discusses how a "journalist" viewed a forwarded copy of an e-mail Professor Lawrence Lessig sent to a friend and somehow interpreted the e-mail erroneously to suggest Lessig was making a sexual proposition. *See* ROSEN, *supra* note 43, at 75-76.

privacy protection.

2. Dignity

Hypothetically, let's assume an employee who sends e-mail over the company network is viewed as having waived any privacy claim regarding the message. Nonetheless, in Montana, unannounced employer monitoring would still probably violate the Constitution's dignity clause, which states in Article II, Section 4, "The dignity of the human being is inviolable."

The dignity clause of the Montana Constitution has been underutilized. In the abortion area, the Montana Supreme Court made one of its rare pronouncements about the clause in dicta:

> Respect for the dignity of each individual – a fundamental right protected by Article II Section 4 of the Montana Constitution – demands that people have for themselves the moral right and moral responsibility to confront the most fundamental questions about the meaning and value of their own lives and the intrinsic value of life in general, answering to their own consciences and convictions.[90]

The central concern is with the arbitrary "denigration and condemnation" of individuals.[91]

It's hard to imagine a greater indignity or degradation than having your personal e-mail read by a supervisor, especially if you have no idea your employer is engaged in this activity. A recent article in the Montana Law Review by Professor Tom Huff and Mathew Clifford suggests the dignity clause should be viewed as covering certain matters that are basic affronts to humanity and yet which other constitutional provisions don't protect.[92] Thus, even if the privacy argument is waived, the Huff/Clifford article reveals a violation of dignity would certainly be a powerful claim. Moreover, an older Montana law review article makes a powerful argument for applying the

90. Armstrong v. State, 1999 MT 261, ¶ 72, 296 Mont. 361, ¶ 72, 989 P.2d 364, ¶ 72.

91. *Id.* ¶ 73.

92. Mathew Clifford & Tom Huff, *Some Thoughts on the Meaning and Scope of the Montana Constitution's Dignity Clause with Possible Applications*, 61 MONT. L. REV. 301 (2000). This article also says that a significant personal degradation must occur to violate the dignity clause. Yet employers may argue that snooping on e-mails that only deal with topics such as what groceries to get for dinner would not suffice. This view, however, is shortsighted because it's simply a happy coincidence for the employee in a certain situation that the uninteresting topic of groceries is involved. Next time, the snooping may reveal very intimate advice the employee's giving to his daughter via e-mail.

dignity clause to private violations.[93] Additionally, there is an interesting law review article, which draws on European legal sources to argue unannounced workplace e-mail monitoring injures the worker's dignity in fundamental ways.[94]

3. Strict Scrutiny

Assuming unannounced workplace e-mail monitoring invades an employee's privacy and dignity rights, the question becomes whether the employer can show its policies are narrowly tailored to promote a compelling interest. The Montana Supreme Court has followed this approach to strict scrutiny in cases like *Siegal*. Two situations might justify surveillance activities of an employer.

First, if the employer has strong evidence that the employee is carrying out a criminal enterprise via e-mail, this would qualify as a compelling interest. Second, if the employer has strong evidence the employee is electronically committing sexual, racial, or other harassment, this activity would likewise justify monitoring. Courts should conclude employers have compelling interests in at least some of these cases so employers aren't in the Catch 22 of being subject to liability if they don't act vigorously to prevent harassment or a crime. An Iowa Law Review article[95] concentrates on the harassment portion of the e-

93. Tia Rikel Robbin, *Untouched Protection from Discrimination: Private Action in Montana's Individual Dignity Clause,* 51 MONT. L. REV. 553 (1989). *See also* Gantt, *supra* note 2.

94. Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace,*19 N.Y.L. SCH. J. INT'L & COMP. L. 379 (2000) (showing how France, Italy, and Europe generally protect electronic privacy in the workplace more comprehensively than the U.S. does in part based on their notions of dignity).

95. Amanda Richman, Note, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 IOWA L. REV. 1337 (2001). This article also shows why the privacy analysis should not generally vary depending on whether the employer is a government agency or a private company. Non-government employers, however, could argue strict scrutiny should not be applied to them. They are likely to argue for a balancing test. They could assert that it does not make sense to discuss whether a *private* employer has a compelling *governmental* interest. Moreover, non-government employees must make a profit – the public interest is secondary. Lastly, Montana's Constitution even refers to the right to earn a living.

But there are several problems with this reasoning. First the Constitutional Convention delegates were very concerned about the dangers of non-governmental intrusions. Second, in *Cape-France Enters.*, the Montana Supreme Court recently used a compelling interest test where the issue involved environmental degradation by a private entity. *Id.*, 2001 MT 139, ¶¶ 31-32, 305 Mont. 513, ¶¶ 31-32, 29 P.3d 1011, ¶¶ 31-32. Third, while the compelling interest test may not be suitable in all Montana cases involving alleged private violations of fundamental rights, the entity disputing the test's applicability should bear a heavy burden of proof to show why it's not suitable.

mail monitoring problem as does much of Professor Rosen's book, *The Unwanted Gaze*.[96]

But even in situations where a criminal enterprise or harassment is being investigated, the examination should be as focused on the specific wrongdoing as possible, rather than be a fishing expedition.[97] These employees still have some privacy rights.[98] Employers should also consider Judge Rosenbaum's recommendation that they give employees some advance notice of an inspection in some instances.

4. Remedies and Preventative Measures

Except for the two limited scenarios mentioned above, e-mail monitoring would seem to be unconstitutional in Montana and should subject the employer to an injunction and appropriate damages. So what should employers do to protect themselves?

Employers should probably take two actions suggested by Nancy Sinclair at the Montana Law Review cyberspace symposium in 1999. First, employers should notify employees that employee e-mail may be monitored, and that employee use of e-mail for personal matters may be problematic.[99] Employees who subsequently expose themselves in e-mails have then knowingly waived their right to privacy. Second, employers should try to have all employees sign user agreements, regarding the computer, in which one provision authorizes monitoring.[100] Through such careful preventative actions,

---

Employers cannot meet that burden, it would seem, regarding e-mail monitoring given the strong privacy and dignity interests.

96. *See supra* note 43.

97. *Id.* at 179-182 (encouraging policy makers to limit electronic searches to serious situations).

98. *See Siegal,* 281 Mont. at 263, 934 P.2d at 183 (stating Montana doesn't necessarily have a compelling interest in enforcing routine criminal laws where significant harms aren't at stake).

99. *Privacy in Cyberspace: Transcripts from the 1999 Judge James R. Browning Symposium*, *supra* note 3, at 64-65.

100. *Id.* Restrictive e-mail monitoring and usage policies, however, are not a panacea for employers. If not carefully drafted, these policies can also be challenged as violating privacy and dignity rights. And if imposed on government employees, these policies can violate free speech rights, particularly as applied to academics doing research where the free speech interest deserves the highest protection. *See e.g.* Kate Williams, Note, *Loss of Academic Freedom on the Internet: The Fourth Circuit's Decision in Urofsky v. Gilmore*, 21 REV. LITIG. 493 (Spring 2002); Donald T. Weidner, *Thoughts on Academic Freedom and Beyond*, 33 U. TOL. L. REV. 257 (2001); *Recent Cases*, 114 HARV. L. REV. 1414 (2001). *But see* Urofsky v. Gilmore, 216 F.3d 401 (4th Cir. 2000), *cert. denied*, 531 U.S. 1070 (2001).

employers can prevent the nightmare of exposure to the types of constitutional claims I have alluded to, and employees will be fully informed.

One downside of this approach is some prospective employees could either refuse to sign an agreement, or refuse to work for an employer who complies with this advice. Given the fact Montana employers can only discharge workers for cause, there may also be issues about whether current employees can be required to sign. After all, what would be the penalty? At a minimum, employers should give employees adequate time and opportunity to read and think about the user agreement. As the above discussion shows, the issue of e-mail monitoring may well pose some fascinating questions for the Montana Supreme Court.

II. PERSONAL JURISDICTION IN CYBERSPACE

An American Bar Association journal article jokingly stated cyberspace personal jurisdiction law is based on the "Missouri rules:"[101] the Missouri party always prevails.[102] This assessment may be harsh given that one should expect the global and ephemeral Internet to create problems for an area of law where state sovereignty remains important. But this ABA article is certainly correct that courts have not been consistent.

The first part of this section discusses the key U.S. Supreme Court cases on personal jurisdiction. The next part examines several Ninth Circuit decisions regarding personal jurisdiction in cyberspace, with a special focus on the sliding scale test and the effects test. The third part critically examines the Montana Supreme Court's foray into this area. Lastly, I provide recommendations on how clients can limit liability.

A. The U.S. Supreme Court

According to the U.S. Supreme Court, there are two kinds of personal jurisdiction: general and specific.[103] General

101. Robert W. Hamilton & Gregory A. Castanias, *Tangled Web: Personal Jurisdiction and the Internet*, 24 LITIG. 27 (1998).

102. *Compare* Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd*, 126 F.3d 25 (2d Cir. 1997) (Missouri defendant not subject to jurisdiction) *with* Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996) (Missouri court had jurisdiction over California defendant in Web trademark case).

103. Helicopteros Nacionales de Colombia, S.A. v. Hall, 466 U.S. 408, 414-415 (1984).

jurisdiction means the courts of a state can adjudicate any claim brought against the defendant, regardless of the subject matter.[104] A defendant must have "continuous and systematic" contacts with the forum state to be subject to general jurisdiction.[105] This requirement is difficult to meet. For example, the U.S. Supreme Court found this test was not satisfied in a case where a non-resident engaged in four million dollars of business with a state.[106] According to the Court, part of the problem was the defendant lacked a persistent physical presence.[107]

Specific jurisdiction exists where three requirements are met. First, the defendant must have "minimum contacts" with the forum state.[108] To put it another way, the defendant must have "purposefully availed" itself of the chance to do business there.[109] Second, the claim must arise out of, or relate to, the defendant's contacts with the forum state.[110] Third, it must be reasonable or fair to assert jurisdiction over the defendant.[111] To determine reasonableness, courts should look at the burden on the defendant, the forum state's interest, the plaintiff's interest, "the interstate judicial system's interest in obtaining the most efficient resolution of controversies; and the shared interest of the several States in furthering fundamental substantive social policies."[112]

The Court has not always been clear about what these requirements mean. In *Asahi Metal Indus. Co. v. Superior Court,*[113] the Court divided on the level of foreseeability required to constitute purposeful availment. *Asahi* involved the issue of whether California courts had personal jurisdiction over a Japanese company that was being sued by a Taiwanese tire tube manufacturer because of an allegedly defective tube valve.[114] A

104. *Id.* at 414-415.

105. *Id.* at 415 (quoting Perkins v. Benguet Consol. Mining Co., 342 U.S. 437, 438 (1952)).

106. *Id.* at 411.

107. *Id.* at 418.

108. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 291 (1980).

109. Hanson v. Denckla, 357 U.S. 235, 253 (1958). *See also International Shoe*, 326 U.S. at 319.

110. *Helicopteros*, 466 U.S. at 415.

111. Asahi Metal Indus. v. Superior Court, 480 U.S. 102 (1987).

112. *World-Wide Volkswagen*, 444 U.S. at 292. *See also* Kulko v. Cal. S. Ct., 436 U.S. 84, 93, 98 (1978).

113. 480 U.S. 102 (1987).

114. 480 U.S. at 105.

California plaintiff had initiated the lawsuit but settled before trial.[115] The Court ruled California lacked jurisdiction because it would be unfair to force a foreign corporation to defend against a foreign plaintiff in such circumstances.[116]

Regarding purposeful availment, Justice Brennan reasoned the Japanese company did enough business in California so that it should reasonably have foreseen the possibility of being sued in the state of California.[117] Justice O'Connor suggested, however, additional actions were required for establishing personal jurisdiction. Justice O'Connor opined the personal jurisdiction threshold may have been met if there was evidence indicating the Japanese company intended for its valves to end up in California, rather than simply knowing the valves might end up there.[118] Her view has been called the "additional conduct test."[119] This disagreement over personal jurisdiction has never been resolved and is significant for the cyberspace issue.[120]

The Supreme Court has also found jurisdiction to exist under the "effects test" adopted in *Calder v. Jones*.[121] In *Calder*, the Court held California courts had jurisdiction over the National Enquirer (based in Florida) for publishing a libelous article about the actress Shirley Jones.[122] The Court reasoned jurisdiction existed because the Enquirer should have known that it would injure Ms. Jones in Hollywood circles.[123] National distribution of the magazine did not eliminate purposeful availment towards California.

B. The Ninth Circuit

As shown above, personal jurisdiction has centered on whether the defendant is sufficiently "present" within the forum state. However, the ephemeral nature of cyberspace raises the

115. *Asahi*, 480 U.S. at 106.

116. *Id.* at 108.

117. *Asahi,* 480 U.S. at 119.

118. *Id.* at 112.

119. Lesnick v. Hollingsworth & Vose Co., 35 F.3d 939, 945 (4th Cir. 1994).

120. The lower courts are divided as between the approaches of Brennan and O'Connor. *See* RICHARD FREER & WENDY PERDUE, CIVIL PROCEDURE 94 (2d ed. 1997). Similarly, courts are divided over whether to take a broad or restrictive view of jurisdiction over web sites.

121. 465 U.S. 783, 789-790 (1984).

122. *Calder*, 465 U.S. at 786.

123. *Id.* at 788.

question: "Is There a There There?"[124] A Web site is both everywhere and nowhere at the same time. Thus, the issue remains: how should personal jurisdiction work in such a situation? Several Ninth Circuit decisions have addressed this question.

1. Cybersell, Inc. v. Cybersell, Inc.[125]

a. The Case

Cybersell involved a trademark infringement action brought by an Arizona corporation, Cybersell, Inc., against a Florida corporation that had initially adopted the same name.[126] Both companies had Web sites.[127] Cybersell, Inc. filed suit in an Arizona federal court.[128] The Arizona company was established in 1994 to provide Internet advertising and marketing services.[129] The company's founders were the first Web users to "spam" the Internet.[130] The Florida company was established in the summer of 1995 and it advertised Web construction services.[131] The Florida company designed its Web site without knowledge of the Arizona company.[132] The Florida company sought declaratory relief as a defense.[133]

The Ninth Circuit ruled the Florida company was not subject to personal jurisdiction in Arizona. The Court initially discussed two cases. In *CompuServe Inc. v. Patterson,*[134] the Sixth Circuit ruled Ohio had jurisdiction over a Texas defendant who traded computer software via an Ohio Internet service provider's network. In *Bensusan Restaurant Corp. v. King,*[135] a New York federal district court found that New York lacked jurisdiction over a Missouri defendant. The plaintiff owned a

124. Michael Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2001).

125. 130 F.3d 414 (9th Cir. 1997).

126. *Cybersell*, 130 F.3d at 415.

127. *Id.*

128. *Id.*

129. *Id.*

130. *Id.*

131. *Cybersell*, 130 F.3d at 415.

132. *Id.* (Perhaps because the Arizona company's site was down for reconstruction after February of 1995).

133. *Id.* at 415-16.

134. 89 F.3d 1257 (6th Cir. 1996).

135. 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd*, 126 F.3d 25 (2d Cir. 1997).

New York jazz club, the "Blue Note," and was suing the owner of a Missouri club, also called the "Blue Note." The Court said the defendant could not be sued in New York because, "Creating a site, like placing a product into the stream of commerce, may be felt nationwide-or even worldwide-but, without more, it is not an act purposefully directed to the forum state."[136]

After discussing these approaches, the Ninth Circuit in *Cybersell* adopted the "sliding scale" test used by the federal district court in *Zippo Mfg. Co. v. Zippo Dot Com, Inc.* Specifically, the Court in Cybersell stated, "In sum, the common thread, well stated by the district court in *Zippo,* is that 'the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet.'"[137] *Zippo* distinguished between Web sites where business was being done in a state (jurisdiction presumptively exists), interactive Web sites (less clear), and passive Web sites (jurisdiction generally doesn't exist).[138]

The Ninth Circuit elaborated by suggesting:

> 'Interactive' web sites present somewhat different issues. Unlike passive sites. . .users can exchange information with the host computer when the site is interactive. Courts that have addressed interactive sites have looked to the 'level of interactivity and commercial nature of the exchange of information that occurs on the Web site' to determine if sufficient contacts exist to warrant the exercise of jurisdiction.[139]

Applying the *Zippo* sliding scale, the Ninth Circuit ruled the Florida company had an essentially passive Web page, did not encourage Arizonans to use the site, did not aim its activities at Arizonans, and apparently received no Arizona "hits" except from the plaintiff.[140] Moreover, the Florida company "entered into no contracts in Arizona, made no sales in Arizona, received no telephone calls from Arizona, earned no income from Arizona, and sent no messages over the Internet to Arizona."[141] The court added Cybersell, FL did not have an 800 number and, "[t]he interactivity of its web page is limited to receiving the browser's name and address and an indication of interest–signing up for

136. *Id.* at 301.

137. *Cybersell*, 130 F.3d at 419 (quoting Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997)).

138. *Zippo*, 952 F. Supp. at 1124.

139. *Cybersell*, 130 F.3d at 419.

140. *Id.*

141. *Id.*

the service is not an option. . ."[142]

The Ninth Circuit then asserted, "Cybersell FL has done no act and has consummated no transaction, nor has it performed any act by which it purposefully availed itself of the privilege of conducting activities, in Arizona, thereby invoking the benefits and protections of Arizona law."[143] The Ninth Circuit further concluded "so far as we are aware, no court has ever held that an Internet advertisement alone is sufficient to subject the advertiser to jurisdiction in the plaintiff's home state."[144] The Court concluded the plaintiff failed to meet the first prong of the specific jurisdiction test (minimum contacts/purposeful availment) and if the Court were to rule differently, "every complaint arising out of alleged trademark infringement on the Internet would automatically result in personal jurisdiction wherever the plaintiff's principal place of business is located . . . ."[145]

The Ninth Circuit found that *Calder*'s effects test was inapplicable because the Florida defendant's Web page "simply was not aimed intentionally at Arizona knowing that harm was likely to be caused there to Cybersell AZ."[146] Moreover, the Court reasoned the effects test could not be applied because corporate defendants do not "suffer harm in a particular geographic location in the same sense that an individual does."[147] Finally, the Ninth Circuit found *Panavision Int'l v. Toeppen*[148] inapplicable.[149]

Cybersell is an example of one of the many courts adopting the *Zippo* sliding scale analysis. A commentator has suggested:

---

142. *Id.*

143. *Cybersell*, 130 F.3d at 419.

144. *Id.* at 418. This statement is debatable given the case of *Inset Sys., Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161 (D. Conn. 1996). A brief discussion of this controversial statement in *Cybersell* can be found in: Mark Kende, *Lost in Cyberspace: The Judiciary's Distracted Application of Free Speech and Personal Jurisdiction Doctrines to the Internet*, 77 OR. L. REV. 1125, 1166 n.231 (1998). One commentator has suggested courts that adopt a very liberal approach to finding jurisdiction over Web sites are using a "spider" approach (wherever the Web goes), whereas courts using a more restrictive test are using a "highway" approach (requiring a more concrete connection). Joseph S. Burns & Richard A. Bales, *Personal Jurisdiction and the Web*, 53 ME. L. REV. 29, 31 (2001). This is analogous to the Brennan/O'Connor division in *Asahi Metal Indus. v. Superior Court*.

145. *Cybersell*, 130 F.3d at 420.

146. *Id.*

147. *Cybersell*, 130 F.3d at 420.

148. 938 F. Supp. 616 (C.D. Cal. 1996), *aff'd*, 141 F.3d 1316 (9th Cir. 1998).

149. *Cybersell*, 130 F.3d at 420.

> The most notable commonality among the Internet jurisdiction cases is their use of precedent. Beginning in March 1997, only two months after the Western District of Pennsylvania laid down the *Zippo* opinion, every district court examining on-line contacts cited to *Zippo*, even though *CompuServe* offered a valid circuit court decision on the issue. District courts continued to cite to *Zippo* throughout 1998 and 1999, despite the fact that by the end of 1999, six circuit court decisions from five different circuits had issued relevant opinions. Highlighting this structural problem is the fact that the districts did not cite *Zippo* as a mere example; most relied almost exclusively on that case as the basis of their analysis and by early 1998 only cited the circuit decisions as mere sample fact patterns to illustrate the logic of *Zippo*.[150]

b. Criticism

Professor Michael Geist, a leading Internet scholar, has dissected the problems with the *Zippo* sliding scale approach. These include the following:

> 1) Most Web sites fall into the middle category of being somewhat interactive and *Zippo* provides little guidance on how to resolve those cases.
>
> 2) A judicial determination that a site is highly interactive doesn't look at the owner's forum state sales, and thus ignores the purposeful availment requirement.
>
> 3) A court might characterize chat room postings as passive, yet defamatory postings have subjected their authors to personal jurisdiction.
>
> 4) Sites may not be what they seem. Apparently passive sites may use hidden data collection technologies.[151]

Another problem is the willingness of courts using the sliding scale approach to examine whether the site had lots of hits in the state. Purposeful availment analysis should focus on what the Web site owner intended, not on the fortuitous circumstance of whether lots of hits in the state occurred.

2. Panavision Intern., L.P. v. Toeppen[152]

The next major Ninth Circuit case involved an appeal of the

150. Christine G. Heslinga, Note, *The Founders Go On-Line: An Original Intent Solution to a Jurisdictional Dilemna*, 9 WM. & MARY BILL RTS. J. 247, 264-65 (2000) (listing appellate court cases). *Accord* Roy N. Dreben & Johanna L. Werbach, *Top 10 Things to Consider in Developing an Electronic Commerce Web Site*, COMPUTER LAWYER, May 1999, at 17, 19 (stating that Internet jurisdiction "appears to be coalescing" around the "seminal *Zippo* case").

151. Geist, *supra* note 124, at 1375-1381.

152. 141 F.3d 1316 (9th Cir. 1998).

district court's decision in *Panavision*. It is worth noting that a commentator has argued *Panavision* is inconsistent with *Cybersell*.[153] Moreover, other courts appear to be divided on whether to follow *Panavision*. This section will analyze the controversial case.

Panavision is a California based company that manufactures motion picture camera equipment.[154] In December of 1995, Panavision sought to register a Web site on the Internet.[155] However, the company discovered that Dennis Toeppen had already used its trademark as the domain name for his Web site.[156] Mr. Toeppen lived in Illinois and had registered the name with Network Solutions, Inc (NSI).[157] NSI registers names on a first come first served basis for a $100 registration fee.[158] Panavision's counsel in California sent Toeppen a letter in Illinois telling him to cease using the name.[159] Toeppen sent a letter back to Panavision in California refusing to give up the name unless Panavision paid him $13,000.[160] After Panavision refused, Toeppen registered Panavision's other trademark, Panaflex, as a domain name and set up a Panaflex Web page that said "Hello."[161] Panavision then filed suit in a California federal court alleging that Toeppen stole domain names and trademarks, and tried to extort money from their rightful owners.[162] The district court found jurisdiction and the Ninth Circuit affirmed.[163]

The Ninth Circuit began its analysis by discussing how *Cybersell* ruled that merely advertising on a web site without "something more" could not create jurisdiction.[164] The Ninth Circuit further stated the *Calder* effects test had not been applicable in *Cybersell*.[165] However, the Ninth Circuit said that the effects test had correctly been the key to the district court

153. Heslinga, *supra* note 150, at 261.
154. *Toeppen*, 141 F.3d at 1319
155. *Id.*
156. *Id.*
157. *Id.* at 1318.
158. *Id.* at 1319.
159. *Toeppen*, 141 F.3d at 1319.
160. *Id.*
161. *Toeppen*, 141 F.3d at 1319.
162. *Id.*
163. *Id.* at 1318.
164. *Id.* at 1321.
165. *Id.*

ruling against Toeppen.[166]

Toeppen argued he had "not directed any activity toward Panavision in California, much less 'entered' the state. . . . [A]ll he did was register Panavision's trademarks on the Internet and post Web sites using those marks; [and] if this activity injured Panavision, the injury occurred in cyberspace."[167] The Ninth Circuit responded by saying that "the present case is akin to a tort case"[168] and that:

> Toeppen engaged in a scheme to register Panavision's trademarks as his domain names for the purpose of extorting money from Panavision. His conduct, as he knew it likely would, had the effect of injuring Panavision in California where Panavision has its principle place of business and where the movie and television industry is centered.[169]

It is fair to say the Ninth Circuit in *Panavision* used the *Calder* effects test, not the *Zippo* sliding scale. However, *Cybersell* was not contradicted in the *Panavision* opinion. The facts in *Cybersell* didn't warrant use of the effects test, unlike the facts presented in *Panavision*. Thus, the commentator who suggested the decisions were contradictory was wrong.[170] One can still debate whether usage of the effects test was proper in *Panavision* but there is no inconsistency with *Cybersell*.

3. *Bancroft & Masters, Inc. v. Augusta Nat'l Inc.*[171]

a. *The Case*

The Ninth Circuit's most recent cyberspace jurisdiction decision takes a novel approach receiving national attention.[172] The plaintiff, Bancroft & Masters, Inc. (B&M), is a small California company selling computer and networking products mainly in the San Francisco area.[173] The defendant, Augusta National Inc. (ANI), operates the Augusta National Golf Club in

166. *Toeppen*, 141 F.3d at 1321.

167. *Id.* at 1322.

168. *Toeppen*, 141 F.3d at 1321.

169. *Id.* at 1322.

170. *See supra*, note 150. The William and Mary Bill of Rights Law Journal article also incorrectly describes a Third Circuit decision as saying Cybersell and Panavision were in conflict. Yet, the Third Circuit expressly stated otherwise. *See* Indus., Inc. v. Kiekert AG, 155 F.3d 254, 264 n.7 (3d Cir. 1998).

171. 223 F.3d 1082 (9th Cir. 2000).

172. Geist, *supra* note 124.

173. *Bankcroft & Masters*, 223 F.3d at 1084.

Georgia where the annual Masters Tournament is held.[174]

B&M alleged ANI sent a letter to the Internet domain name registry's Virginia headquarters (NSI) challenging B&M's use of the domain name, masters.com.[175] ANI also sent a letter to B&M in California demanding B&M cease and desist using the domain name and transfer it immediately to ANI.[176] Based on these and other actions by ANI, B&M sued ANI in the Northern District of California seeking a declaratory judgement.[177] The California federal court concluded it lacked personal jurisdiction over ANI.[178] However, on appeal, the Ninth Circuit reversed this finding.[179]

The Ninth Circuit concluded there was an "express aiming" requirement to the *Calder* effects test, which had to be satisfied, namely the defendant must "have engaged in wrongful conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state."[180] After discussing several cases, the Court stated, "The presence of individualized targeting is what separates these cases from others in which we have found the effects test unsatisfied."[181] In *Cybersell*, for example, there was no showing "the defendants even knew of the existence of the plaintiffs, let alone targeted them individually."[182] In summary, the Court ruled in *Bancroft & Masters* that the defendant must have "(1) committed an intentional act, which was (2) expressly aimed at the forum state, and (3) caused harm, the brunt of which is suffered and which the defendant knows is likely to be suffered in the forum state."[183]

The Ninth Circuit then analogized *Bancroft* to the intentional tort scheme at issue in *Panavision*:

> Applying these concepts to the instant case, we conclude that B&M has demonstrated purposeful availment by ANI under the *Calder* effects test. ANI acted intentionally when it sent its Letter to NSI. The letter was expressly aimed at California because it individually targeted B&M, a California corporation doing

174. *Id.*

175. *Id.* at 1085.

176. *Id.*

177. *Id.* (In their declaratory judgment, B & M requested the Court to find non-dilution and non-infringement).

178. *Bankcroft & Masters,* 223 F.3d at 1085.

179. *Id.* at 1089.

180. *Bankcroft & Masters,* 223 F.3d at 1087.

181. *Id.* at 1088.

182. *Id.*

183. *Id.* at 1087.

> business almost exclusively in California. Finally, the effects of the letter were primarily felt, as ANI knew they would be, in California.[184]

b. Criticisms of Bancroft's Express Aiming

One problem with *Bancroft's* targeting approach is *Calder* was an intentional tort case and *Bancroft* is not. The concurring opinion showed its awareness of this problem by stating, "I concur in the opinion only on the assumption that Augusta National, through its letter to NSI, engaged in tortious conduct, i.e., that they intended to effect a conversion of the masters.com name."[185] Yet the district court disagreed, stating, "No such intentional scheme or tortious conduct is alleged in this action."[186]

A further problem with *Bancroft*, according to a commentator, is that it's doubtful *Calder* involved a publication intending to injure Shirley Jones. Presumably, the Enquirer instead sought to attract readers.[187] Thus, the majority's requirement in *Bancroft,* that the defendant intend to harm the plaintiff in the forum state, need not be read so strictly. It should be enough that the defendant has knowledge a tortious effect is likely to occur, not that the defendant intended the tortious effect for a specific state.

This same commentator argues *Bancroft* was wrong, even under a more liberal effects test. He suggests:

> The result of the majority opinion seems unfair because while Bancroft had agreed to NSI's dispute resolution procedure concerning the "masters.com" domain name, Augusta had not. Subjecting a defendant to personal jurisdiction in the forum state on the basis of contractual relations between the plaintiff and a third party is unjust.[188]

Yet this powerful objection does not undermine the targeting legal principles. The objection says they were misapplied.

---

184. *Bancroft & Masters*, 223 F.3d at 1087.

185. *Id.* at 1089.

186. Bancroft & Masters, Inc. v. Augusta Nat'l., Inc., 45 F. Supp. 2d 777, 782 (Cal. 1998). The district court also ruled, "The intellectual property dispute underlying the instant complaint does not 'arise out of' ANI's letter to Network Solutions, Inc.", thus failing another prong of the specific jurisdiction test. *Id.*

187. Christopher Allen Kroblin, Note, *Expanding the Jurisdictional Reach for Intentional Torts: Implications for Cyber Contacts*, 31 GOLDEN GATE U. L. REV. 51, 87 n.251 (2001).

188. Kroblin, *supra* note 187, at 87.

c. The Benefits and Unanswered Questions Regarding Targeting

Professor Michael Geist has said *Bancroft's* "express aiming" or "targeting" focus is a superior approach to cyberspace jurisdiction questions because it avoids the weaknesses of *Zippo*. He says:

> Unlike the *Zippo* approach, a targeting analysis would seek to identify the intentions of the parties and to assess the steps taken to either enter or to avoid a particular jurisdiction. Targeting would also lessen reliance on effects-based analysis, the source of considerable uncertainty since Internet-based activity can ordinarily be said to create some effects in most jurisdictions.[189]

Professor Geist then elaborates on what aspects of the targeting test need to be fleshed out, after showing how it's increasingly being advocated by courts and commentators. His discussion has special power after seeing the misapplication of the test in *Bancroft*:

> To identify the appropriate criteria for a targeting test, we must ultimately return to the core jurisdictional principle – foreseeability. Foreseeability should not be based on a passive versus active Web site matrix, however. Rather, an effective targeting test requires an assessment of whether the targeting of a specific jurisdiction was itself foreseeable. Foreseeability in that context depends on three factors – contracts, technology, and actual or implied knowledge. Forum selection clauses found in Web site terms of use agreements or transactional clickwrap agreements allow parties to mutually determine an appropriate jurisdiction in advance of a dispute . . . . Newly-emerging technologies that identify geographic location constitute the second factor. These technologies, which challenge widely held perceptions about the Internet's architecture, may allow sites to target their content by engaging in "jurisdictional avoidance." The third factor, actual or implied knowledge, is a catch-all that incorporates targeting knowledge gained through the geographic location of tort victims, offline order fulfillment, financial intermediary records, and Web traffic.[190]

Professor Geist concludes, "[t]he move toward using contract and technology to erect virtual borders may not answer the question of whether there is a there there, but at least it will go a long way in determining where the there might be."[191] The American Bar Association in a recent study reported favorably

189. Michael Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 661 PRAC. L. INST. PAT. 561, 598 (July 2001).

190. Geist, *supra* note 189, at 602-03.

191. *Id.* at 624.

on the targeting approach as well.[192] Thus, this seems to be the cutting edge of cyberspace jurisdiction theory.

C. The Montana Cases

1. The Cases

The leading Montana Supreme Court decision regarding cyberspace personal jurisdiction is *Bedrejo v. Triple E Canada, Ltd.*[193] The case involved a Canadian manufacturer of a motor home that crashed while being driven near Dillon, Montana.[194] The driver and passengers were foreigners and were all either killed or injured.[195] Concerning jurisdiction, plaintiffs argued Triple E had a Web site accessible in Montana, advertised in national magazines, ran an "Adventure Club" to plan trips through the U.S. and Canada, and owned out-of-state dealerships providing sales coverage for at least three Montanans.[196] Triple E responded, however, that the company was not registered with the Montana Secretary of State, and that the company did not have an office, a phone listing, any employees or any dealers in Montana.[197] The motor home also was purchased outside of Montana.[198]

The Montana Supreme Court affirmed the district court's decision finding Montana lacked personal jurisdiction.[199] The Court said the plaintiff made no clear allegations the claims arose out of or were related to Triple E's contacts with the forum state.[200] Thus, specific jurisdiction was lacking.

The Court further determined Triple E's Web site did not establish jurisdiction.[201] The Court relied on *Bensusan Restaurant Corp. v. King* and another non-Montana case,

192. GLOBAL CYBERSPACE JURISDICTION PROJECT, AM. BAR ASS'N, A REPORT ON GLOBAL JURISDICTION ISSUES CREATED BY THE INTERNET 28-30 (London Meeting 2000), *available at* http://www.abanet.org?buslaw/cyber/initiatives/draft.rtf.

193. 1999 MT 200, 295 Mont. 430, 984 P.2d 739.

194. *Bedrejo*, 1999 MT 200, ¶ 3.

195. *Id.* at ¶¶ 3-4.

196. *Id.* at ¶ 8.

197. *Id.* at ¶ 11.

198. *Bedrejo*, 1999 MT 200, ¶ 11.

199. *Id.* at ¶ 21.

200. *Id.* at ¶ 15. Specifically, the Court stated "Nothing was presented to connect the victims or the driver of the motor home with any of these 'contacts' between Montana and Triple E." *Id.*

201. *Id.* at ¶¶ 17-20.

Millennium Enterprises Inc. v. Millennium Music, LP.[202] There, an Oregon federal court held an interactive Web site did not expose its owner to liability in Oregon unless it could be shown that Oregon residents actually consummated transactions through the site in sufficient numbers.[203] Similarly, the Montana Supreme Court concluded *Bedrejo* by stating, "We agree with the District Court that any 'entry' by Triple E into Montana amounted to only an 'insignificant trickle' in the stream of commerce, and we hold that the exercise of jurisdiction over Triple E would not be reasonable."[204]

Apart from *Bedrejo*, The Montana Supreme Court briefly touched on the issue of cyberspace personal jurisdiction in *Threlkeld v. Colorado*.[205] In *Threlkeld*, the Court cited approvingly to *Bedrejo* in its discussion about why general jurisdiction was absent.[206] *Threlkeld* involved a lawsuit by some Montanans alleging veterinary malpractice against Colorado State University.[207] The Court said there was nothing to indicate that CSU's Web site "is anything more than a medium for the dissemination of information to Internet users."[208] Thus, CSU could not be subject to personal jurisdiction based on the Web site.[209] Interestingly, the Montana Supreme Court in *Threlkeld* did not discuss *Bedrejo* when determining specific jurisdiction was lacking over CSU.

2. *Assessing Bedrejo*

Bedrejo suggests the Montana Supreme Court is hesitant to expose out-of-staters to jurisdiction in Montana based solely on Web sites. For example, Professor Geist cites *Millennium Enterprises* as one of the leading cases critical of the supposedly amorphous *Zippo* test.[210] Geist also approvingly cites *Bensusan* as a case protecting Internet business activity.[211]

---

202. Id. at ¶ 20; *see Bensusan*, 937 F. Supp. 295 (S.D.N.Y. 1996) and *Millennium*, 33 F. Supp. 2d 907 (D. Or. 1999).

203. *Millennium*, 33 F. Supp. at 921. This analysis is troubling because the number of hits in the state doesn't determine whether the Web site owner purposefully availed himself of the chance to do business there or not.

204. *Bedrejo*, 1999 MT 200, ¶ 21.

205. 2000 MT 369, 303 Mont. 432, 16 P.3d 359.

206. *Id.* at ¶ 16.

207. *Id.* at ¶¶ 3- 4.

208. *Id.* at ¶ 17.

209. *Id.*

210. Geist, *supra* note 124, at 1376.

211. *Id.* at 1365.

On the other hand, *Bedrejo* may only have limited precedential value since the Court was distracted by the Web jurisdiction issue and engaged in a flawed specific jurisdiction analysis. Courts are frequently distracted from applying normal legal principles in cyberspace cases.[212] How was the Court's ruling in *Bedrejo* flawed and distracted?

First, the Supreme Court ignored several Montana federal district court decisions holding that a defendant who commits a tort in Montana is subject to personal jurisdiction in a lawsuit arising out of or related to that tort. For example, in *Great Plains Crop Mgmt. Inc. v. Tryco Mfg. Co.*,[213] the Court stated:

> a manufacturer should be expected to defend its products whenever they go, when that manufacturer intends distribution beyond a purely local level. [*Scanlan v. Normal Projektil Fabrik; Yules v. General Motors Corp.*] While *Scanlan* was a Rule 4B(1)(b) "tort accrual" case, the same principle applies here: a party seeking the advantages of a broader marketing area must be expected to follow those products. The defendant knew its products were going to Montana. It should also have known that problems could develop.[214]

Yules v. General Motors Corporation even involved an auto crash where the court rejected the car manufacturer's motion to dismiss for lack of personal jurisdiction.[215] While the Montana Supreme Court is not bound by these federal court rulings, failing to discuss them is bad form.

Second, the Montana Supreme Court also never mentions the most analogous U.S. Supreme Court case on personal jurisdiction, namely *World Wide Volkswagen v. Woodson*.[216] The Court there analyzed whether Oklahoma had personal jurisdiction over a New York area car dealer that sold a car which subsequently exploded in Oklahoma.[217] The Court found the New York dealer had not purposefully availed itself of the chance to do business outside the tri-state area where it made

---

212. *See* Mark S. Kende, *Lost in Cyberspace: the Judiciary's Distracted Application of Free Speech and Personal Jurisdiction Doctrines to the Internet*, 77 OR. L. REV. 1125 (Winter 1998).

213. 554 F. Supp. 1025 (D. Mont. 1983).

214. *Great Plains*, 554 F. Supp. at 1028 (citations omitted). The Court cited *Scanlan v. Normal Projektil Fabrik*, 345 F.Supp. 292, 293 (D. Mont. 1972) and *Yules v. General Motors Corp.*, 297 F. Supp. 674 (D. Mont. 1969).

215. *See also* Thompson v. Chrysler Motors Corp., 755 F.2d 1162, 1172 (5th Cir. 1985).

216. 444 U.S. 286, 287.

217. *Id.* at 288.

most of its sales.[218] The Court, however, kept the German car manufacturer in the case because of its global sales and marketing efforts.[219] Similarly, there's at least some evidence in the *Bedrejo* record suggesting Triple E marketed and serviced its motor homes throughout the United States.[220]

Third, the Court in *Bedrejo* also mistakenly insisted the lawsuit didn't arise out of the Triple E Web page, or any of Triple E's other contacts. However, the lawsuit obviously arose out of Triple E's most significant contact with the state: the motor home's presence there. Indeed, the Triple E Web site should almost be irrelevant to the analysis given this crucial connection.

In conclusion, though *Bedrejo* suggests the Montana Supreme Court will not find personal jurisdiction to exist based solely on a Web site, the decision is not the most convincing precedent.[221] The Court seems to adopt a *Zippo* sliding scale test with the added requirement that the lawsuit must arise directly out of any Web site interactivity with the forum state. The problem is the case seems inconsistent with U.S. Supreme Court precedents like *World Wide Volkswagen,* even without regard to the Internet issue. Perhaps this is why the Montana Supreme Court in *Threlkeld* conducted its specific jurisdiction analysis without mentioning *Bedrejo*.

D. Recommendations

The above analysis above shows the great uncertainty existing over cyberspace personal jurisdiction. What advice then should clients receive to limit liability? The following is a list of suggestions I told attorneys in a recent Continuing Legal Education program:

> 1) Advise your clients about the risks of having a highly interactive Web site shown by *Zippo* and the cases just discussed.
>
> 2) Advise your clients to be careful about posting messages on their Web sites directed at attracting customers from any particular state or locale. Such messages give customers in those locations the ability to argue your client targeted that jurisdiction.

---

218. *Id.* at 295.

219. *World Wide Volkswagen,* 444 U.S. at 314.

220. *See Bedrejo*, 1999 MT 200, ¶ 8.

221. The decision is also internally contradictory. The Court quoted plaintiff's complaint as saying magazine ads were distributed in Montana, but later says there was no proof that the magazines were available in Montana. *Bedrejo*, 1999 MT 200, ¶ 8, ¶ 12.

3) Recommend to your clients they insert "choice of forum" and "choice of law" clauses into Web site order forms. The clauses should also be highlighted to weaken adhesion contract objections.

4) Recommend to your clients they determine how much business their Web site generates per state. Based on this information, you can provide information about whether those states have broad or narrow approaches towards cyberspace jurisdiction. For example, the Northern District of Illinois seems to have a broad approach, unlike the Eastern District of Pennsylvania.[222]

5) Recommend to your clients any Internet message they post or send should contain a disclaimer saying it is only intended to be read by viewers in those states where the message is legal.

6) Remind your clients the substantive law may be different in the states where they do business via the Web as compared to Montana's substantive law. They may, therefore, have to change their behavior to avoid liability.

7) Advise your clients to be careful about what they advertise so they can't be subject to fraud or deceptive advertising claims.

8) Advise your clients to be careful about what hypertext links they provide. The links may include defamatory or fraudulent material and your clients could be held responsible.

9) Remind your clients to be careful about allowing employees or anybody else to post information on the Web sites so as to avoid possible liability.

10) Advise your clients to comply with any privacy requirements in the jurisdictions where their Web site can be accessed. This means they may need to be cautious about what tracking they do (*see* recommendation #4 above).

11) Advise your clients about the importance of keeping the Web site current and keeping informed regarding new cyberspace legal and technological developments. For example, new geographic technologies may enable Web sites to block access in certain forums where the site content may be problematic.[223]

CONCLUSION

Cyberspace has raised numerous interesting problems as courts struggle to apply old doctrines to dynamic technology. Though this process will take a while, cyberspace will ultimately test the doctrines, revealing which make sense and which deserve substantial modification. To that extent, cyberspace, in

222. There is, however, a downside to this recommendation. Tracking would prevent your client from claiming ignorance about where it was doing Web business, thus weakening its argument against purposeful availment. Nonetheless, I think such ignorance is not usually persuasive to courts.

223. Geist, *supra* note 124, at 1385.

the long run, will benefit the courts and those who take advantage of all it has to offer.